View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Lirias

Construcción de redes sociales anónimas

Alejandra Silva[1], L. Javier García[1], Claudia Diaz[2]

1. Grupo de Análisis, Seguridad y Sistemas (GASS)
Departamento de Sistemas Informáticos y Programación
Facultad de Informática
Universidad Complutense de Madrid (UCM)
E-mail: asilva@fdi.ucm.es, javiergv@sip.ucm.es

2. K.U.Leuven ESAT/COSIC
E-mail: claudia.diaz@esat.kuleuven.be

***Resumen*—Analizar una red social permite identificar sus líderes, roles y comunidades, así como su comportamiento, tamaño y heterogeneidad. Esta información es muy valiosa para optimizar o personalizar servicios, y para predecir el comportamiento de la red. Pero al mismo tiempo dichos análisis conllevan intrusiones a la privacidad de los individuos que la conforman. En el presente artículo se revisan las técnicas, algoritmos, y procedimientos que se han presentado recientemente en el campo de investigación para la anonimización de redes sociales, a fin de presentar un amplio panorama de lo que se ha propuesto, y los interrogantes que quedan aún por resolver.**

***Palabras clave*— Anonimato (*anonymity*), algoritmos para grafos (*graph algorithms*), análisis de redes sociales (*social networks analysis*), minería de datos (*data mining*), privacidad (*privacy*).**

I. Introducción

En los últimos años se han desarrollado tecnologías que permiten establecer comunidades sociales virtuales, así como trasladar al mundo virtual las comunidades existentes en el mundo real. Estas tecnologías están transformando la manera en que se desarrollan las relaciones sociales, y teniendo un gran impacto en nuestra sociedad.

Diversos investigadores han abordado este tema desde diferentes áreas de interés, entre ellas la mercadotecnia, epidemiología, sociología, criminalística, o terrorismo, entre otras. El análisis de redes sociales se ha facilitado en años recientes gracias al desarrollo de Internet y a la gran cantidad de información disponible.

Analizar la estructura de una red social revela información de los individuos que la componen, ya que al analizar las conexiones entre individuos podemos identificar los roles que tienen en su grupo o comunidad; así como las dinámicas de las relaciones entre individuos. Esta información es de gran utilidad para comprender mejor las dinámicas sociales. Por ejemplo, sociólogos e historiadores desean conocer la interrelación entre los actores sociales o políticos de una determinada red social para identificar agentes de cambio [1]. Otras investigaciones se han enfocado en analizar los envíos de correos electrónicos, con el objetivo de identificar comunidades y observar su comportamiento [2, 3, 4]. Para el análisis de las bitácoras en línea (*blogs)*, se emplean técnicas de inferencia colectiva que predicen el comportamiento de una entidad a través de sus conexiones. Y mediante técnicas de aprendizaje automático o modelos de lenguaje natural [5, 6], se pretende identificar al autor de un texto al realizar un análisis de su vocabulario y manera de escribir. Sin duda las redes sociales en Internet como *MySpace*, *Friendster*, *Match.com*, *FaceBook,* entre otras, han atraído la atención de millones de personas que participan en ellas activamente para establecer contacto con amigos, buscar empleo o pareja, compartir fotos, música, videos, etc. Diversas publicaciones han demostrado la sorprendente cantidad de información personal que usuarios de estos sitios publican, sin que parezca que sean conscientes de los riesgos que conlleva que esa información sea utilizada en otros contextos [12] [13]. Por ejemplo, cuando empresas encargadas de la contratación de personal realizan búsquedas en redes sociales en línea para investigar el perfil de sus candidatos [14].

A raíz de los eventos del 11 de septiembre se legitimó la aplicación de toda clase de herramientas tecnológicas para vigilar y monitorizar a las personas. Desde entonces, muchas naciones han reformado su legislación para permitir la recopilar información relativa al tráfico y la localización de dispositivos electrónicos como teléfonos fijos y móviles, servicios de mensajes cortos, faxes, *e-mails*, salas de conversación en línea, Internet, entre otros [14]. La justificación radica en prevenir, investigar y perseguir actividades ilícitas o delictivas que atenten contra el orden público, la salud o la seguridad nacional. Mientras tanto, la industria argumenta que el conocer los gustos y hábitos de sus clientes les permite mejorar y personalizar sus servicios.

Sin embargo, desde organizaciones que defienden y promocionan derechos relativos a la privacidad se han expresado recelos con respecto a los riesgos asociados a establecer estos mecanismos de vigilancia masiva. En particular, preocupa la falta de transparencia y responsabilidad con respecto al uso que se da a esta información, y los posibles abusos que se puedan derivar de ello. Un caso extremo que ilustra la importancia de proteger esta información lo ofrecen naciones con regímenes totalitarios, donde grupos de disidentes, periodistas, protestantes cívicos, líderes estudiantiles, organizaciones políticas de oposición o precursores de los derechos humanos quedan expuestos y en peligro para su integridad física [15].

Como podemos observar, es necesario establecer mecanismos para permitir a los individuos proteger la información relativa a las redes sociales a las que pertenecen. El objetivo de este trabajo es presentar un estudio del arte de las propuestas que se han desarrollado recientemente, en el campo de la construcción de redes sociales anónimas. En la sección 2 presentamos la relación de las redes sociales con el

anonimato. En la sección 3 se plantean tipos de ataques que deben ser tenidos en cuenta. En la sección 4 se analizan las técnicas, protocolos y algoritmos para construir redes sociales anónimas; y finalizamos este artículo en la sección 5, donde se presentan las conclusiones de este estudio así como los aspectos que requieren más investigación.

II. Formulación del problema

En esta sección formalizamos la definición y el modelado de redes sociales, definimos las brechas de privacidad que se desean impedir, y presentamos los supuestos y el planteamiento del problema.

A. Definición de red social.

Una red social puede representarse a través de un grafo donde los vértices representan a las personas y las aristas son las relaciones entre ellas. Formalmente, una red social se modela como un grafo $G = (V, E)$ donde:

- $V = (v_1,\ldots, v_n)$ es el conjunto de vértices o nodos que representan a entidades o individuos
- E es el conjunto de relaciones sociales entre ellos (representadas como aristas en el grafo) donde $E = \{(v_i, v_j) \mid v_i, v_j \in V\}$.

B. Definición de anonimizar.

Definimos *anonimizar* como el proceso de transformar un grafo G en su equivalente anónimo AG.

C. Brechas de privacidad.

Las brechas de privacidad en la información de redes sociales pueden ser agrupadas en 3 categorías [11]: 1) revelación de identidad (*identity disclosure*): se descubre la identidad de los individuos asociados los vértices; 2) revelación de conexión (*link disclosure*): se descubren las conexiones entre dos vértices; 3) revelación de contenido (*content disclosure*): se compromete la privacidad de los datos coligados con cada vértice. El objetivo de anonimizar una red social es impedir que la identidad, conexiones, y contenido de los vértices sean revelados.

D. Planteamiento del problema.

En [8] se considera el siguiente planteamiento para definir el problema de preservar la privacidad de los datos en una red social publicada:

1) Se debe identificar la información que se desea proteger.
2) Se debe modelar el conocimiento y habilidades del adversario que trata de comprometer la privacidad.
3) Por último, se debe especificar el uso de la red social, de tal manera que se elija un método de anonimato adecuado que preserve la utilidad de la red y proteja su privacidad.

En este artículo consideramos ataques de revelación de identidad, donde el adversario intenta descubrir la correspondencia entre vértices del grafo anónimo y usuarios de la red social. Para los ataques activos y pasivos se asume que el adversario conoce al completo el grafo $G = (V, E)$ de la red social, la cuál es anonimizada a través de *naive anonimization*. Para los ataques de vecindario se asume que el adversario conoce sólo a los vecinos inmediatos de ciertos vértices y cómo están conectados. Las técnicas que se consideran en este trabajo para anonimizar la red son para prevenir la revelación de identidad. El recurso más utilizado para ocultar la correspondencia entre identidades y su correspondencia con los vértices en una red social es añadir y/o eliminar vértices y aristas.

III. Ataques

A. Anonimización inexperta (naive anonymization)

Primero revisamos el proceso de anonimización inexperto conocido en inglés como *naive anonymization* [7]. Consiste simplemente en renombrar los vértices de G con pseudónimos para prevenir la revelación de su identidad, sin modificar la estructura de la red. En este escenario, si el atacante cuenta por anticipado con información estructural de la red, podrá con alta probabilidad relacionar vértices del grafo anónimo con sus correspondientes. Por ejemplo: En la Fig. 1 vemos que Alicia está relacionada con Beto y Carlos, y que ambos tienen dos conexiones. Cuando el atacante observa el grafo anónimo, puede identificar al vértice 1 con Alicia, puesto que es el único con una estructura de conexiones que encaja con la esperada para Alicia.

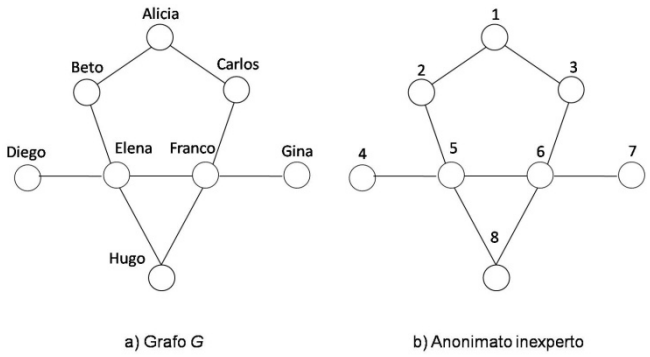

Fig. 1. Ejemplo de anonimato inexperto.

B. Ataques activos.

El objetivo del ataque activo es revelar las identidades de un conjunto de usuarios previamente elegidos. A estos usuarios se les conoce como usuarios víctima b.

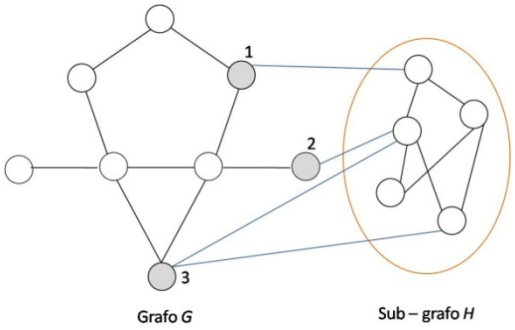

Fig. 2. Ejemplo de ataque activo con $k = 5$ y $b = 3$.

El adversario activo ejecuta los siguientes pasos antes de la anonimización de la red social G: 1) selecciona arbitrariamente un conjunto usuarios víctima $w_1,\ldots, w_b$; 2)

genera k vértices nuevos $X = \{x_1, \ldots, x_k\}$; y 3) crea las conexiones a los usuarios víctima $\{x_i, \ldots, w_i\}$ (por ejemplo enviando mensajes, creando entradas en libretas de direcciones, o alguna otra actividad dependiendo de la naturaleza de la red social). En la Fig. 2 se muestra un ejemplo donde un subgrafo H es insertado en G, con un valor $k = 5$ para un conjunto $\{x_1, \ldots, x_5\}$, y $b = 3$ usuarios víctima $\{w_1, w_2, w_3\}$.

Cuando G sea anonimizada con el modelo *naive anonymization* el atacante podrá identificar H, analizando las aristas de AG, lo que le permite identificar a los usuarios víctima $w_1,\ldots, w_b$ y por lo tanto comprometer su privacidad. El adversario debe construir H con las siguientes propiedades para que sea efectiva: 1) debe ser única en G; 2) debe ser eficientemente localizable; y 3) no debe tener automorfismos

En base al principio de los ataques activos señalado, se presentan dos variantes cuyas diferencias radican en la construcción de H y en los algoritmos aplicados para la recuperación de H en AG.

1) Ataque basado en recorridos (Walk based attack)

Para el primer ataque se muestra que un subgrafo H creado aleatoriamente con $k = \Theta(\log n)$ vértices puede ser identificado en AG con alta probabilidad. Y si el máximo grado de los vértices en H es $\Theta(\log n)$, entonces H puede ser recuperada eficientemente. El algoritmo utilizado para la recuperación de H se llama *walk-based attack*. Consiste en localizar la ruta $x_1, x_2,\ldots, x_k$ en el grafo AG. El proceso inicia haciendo un recorrido vértice por vértice, y verificando la secuencia de grados de los vértices en la ruta para comprobar si coinciden con los esperados para el conjunto X.

Al aplicar este ataque en una red social de 4.4 millones de vértices y 77 millones de conexiones, se destaca que utilizando un valor $k = 7$ puede comprometerse en promedio la identidad de 70 vértices y cerca de 2,400 aristas.

2) Ataque basado en cortes (*cut-based attack*)

El segundo ataque activo llamado ataque basado en cortes también construye H aleatoriamente, pero es insertada en G utilizando muy pocas conexiones. El atacante recupera H a través de cálculos con alta complejidad basados en el modelo de corte de árboles Gumory-Hu. Este ataque utiliza $k = O(\sqrt{\log n})$ para revelar la identidad de $\Theta(\sqrt{\log n})$ vértices víctima. Se muestra que, en el peor de los casos se deben crear al menos de $\Omega(\sqrt{\log n})$ vértices nuevos en cualquier ataque activo que necesite un subgrafo H único e identificable con alta probabilidad.

En la construcción de H denotamos $\delta(H)$ el mínimo grado en H, y γ(H) el valor del mínimo corte en H (número mínimo de conexiones cuya eliminación desconectan a H de G). Para encontrar H se utiliza el algoritmo de corte Gumory-Hu basado, en términos generales en seccionar el grafo iterativamente hasta encontrar un conjunto de vértices isomorfo a H. A diferencia del ataque basado en caminos, la aplicación del algoritmo para la recuperación de H en éste ataque, tiene un alto costo en términos computacionales. Para una red G con 100 millones de vértices, y un valor de $k = 12$, el adversario es capaz de identificar a b = 3 usuarios víctima con probabilidad de al menos 0.99.

C. Ataques pasivos.

El adversario considerado en este ataque es un conjunto de usuarios maliciosos que colaboran a fin de identificar a otros vértices en la red social anónima AG. Cuando AG se publica, los vértices maliciosos tratan de localizarse a sí mismos en la versión anónima de la red social. Esto les permite ubicar sus vértices vecinos y comprometer su identidad. Aplicando un ataque pasivo a la misma red social mencionada en el ataque activo basado en caminos, se obtuvo que si un usuario u es capaz de confabularse con otros $(k - 1)$ vértices vecinos, es capaz de identificar a todos los vértices conectados a ellos. Bajo este criterio se asume que: 1) una confabulación X de tamaño k es iniciada por un usuario que convence a $k - 1$ de sus vecinos; 2) los vecinos confabulados conocen con quién están relacionados dentro de X; 3) los vecinos confabulados conocen los nombres de las entidades con quien están relacionados fuera de X. Debido a que en este caso H no se construye aleatoriamente, no hay bases para considerar que sea única y fácilmente identificable.

El ataque se describe de la siguiente manera:

1) Un usuario x_1 selecciona $k - 1$ vecinos para formar una confabulación de usuarios maliciosos $X = \{x_1, \ldots, x_k\}$
2) Una vez que G es publicado, los usuarios maliciosos ejecutan el algoritmo del ataque basado en caminos con modificaciones mínimas.

Una vez que el grupo de usuarios maliciosos se encuentra en el grafo, les es posible determinar la identidad de algunos de sus vecinos en $G - X$.

D. Diferencias entre ataques pasivos y activos.

Los ataques activos tienen efectos más potentes en la red, ya que el adversario puede elegir los vértices que desea comprometer, siempre y cuando la naturaleza de la red le permita introducir sus vértices en las posiciones deseadas. En cambio, los ataques pasivos solamente pueden revelar la identidad de los vértices que están conectados al atacante (modelado como un grupo de usuarios maliciosos), hecho que garantiza su aplicación en casi cualquier tipo de red. Los ataques pasivos a diferencia de los activos no son fáciles de detectar, por el hecho de que el adversario pertenece a la red social y no genera evidencia de intromisiones externas.

E. Ataque de vecindario.

En [8] se identifica otro ataque a la privacidad en redes sociales llamado ataque de vecindario. En una red social $G = (V, E)$, el vecindario de un usuario $u \in V(G)$ es un subgrafo de vecinos de u que se denota como $Vecindario_G(u) = G(N_u)$ donde $N_u = \{v|(u, v) \in E(G)\}$. Si el atacante conoce a los vecinos de su vértice víctima y sus aristas a otros vértices, puede ser capaz de revelar varias identidades en una red social, aún cuando ésta haya sido modificada a través de técnicas de anonimato. Por ejemplo, supongamos que el atacante cuenta con información estructural del grafo G; sabe que Alicia tiene relación con Beto y Carlos, y que ellos a su vez tienen tres vecinos más; el atacante es capaz de identificar a Alicia y a sus vecinos en la red anónima buscando todos aquellos subgrafos con características similares al suyo.

Para proteger la privacidad satisfactoriamente se propone utilizar el modelo *k-vecindario* anonimato que se detallará en la siguiente sección.

IV. Técnicas, algoritmos y protocolos para la construcción de redes sociales anónimas

Uno de los problemas que se enfrentan en la construcción de redes sociales anónimas es que no se puede considerar cada vértice individualmente, sino que hay que tener en cuenta el grafo en su conjunto, ya que cualquier modificación en un vértice afectará las propiedades del grafo, tales como diámetro, centralidad, heterogeneidad; dando como resultado en la mayoría de los casos una red anónima tan diferente de la original que carece de utilidad.

A. Esquema de encriptación con llave pública.

En [9] presentan una propuesta considerando un escenario en el que múltiples partes tienen una pieza de la red, es decir considera la existencia de "autoridades" que conocen partes del grafo *G*. Se proponen una serie de protocolos criptográficos para transformar *G* en una versión anónima (*AG*), bajo la suposición de que la mayoría de las autoridades son honestas. Se considera que existen autoridades y entidades maliciosas, así como confabulaciones entre ellas. El resultado del proceso de anonimización es un grafo *AG* isomórfico a *G*, y su construcción se realiza a través del conjunto de autoridades de manera que ninguna de ellas es capaz de conocer la relación entre *AG* y *G*.

Para lograr este objetivo se recurre al esquema de encriptación con llave pública ElGamal, que sirve para encriptar la relación entre usuarios y pseudónimos.

Se asume que la red cuenta con conexiones dirigidas no etiquetadas, y se establecen una serie de medidas para evitar ataques por parte de vértices maliciosos que pudieran reportar conexiones específicas para facilitar ataques posteriores. Las medidas preventivas consisten en deshabilitar las etiquetas en las aristas; se eliminan las aristas que van de un vértice a si mismo; limitar las aristas salientes de los vértices (*out-degree*); limitar las aristas entrantes a los vértices (*in-degree*); agregar o eliminar a la red un número aleatorio de aristas y vértices. La selección del protocolo de anonimización se hace de acuerdo con la red, el escenario de aplicación y el objetivo de la transformación.

Para iniciar el proceso de construcción de la red anónima *AG* se permite a cada vértice reportar pseudónimamente sus conexiones en el grafo *G* a las autoridades y se forma una lista *L* de *n* textos cifrados. $E(1),\ldots, E(n)$. Las autoridades que actúan como servidores de mezcla (*mix servers*), ingresan la lista *L*, de la cual resulta una lista con permutaciones $E(\pi(1)),\ldots, E(\pi(n))$. Posteriormente, para ocultar el número de aristas que reportó cada vértice se añaden *n* elementos más a la lista con valor $E(-1)$ de tal manera que la lista *L'* resultante contenga *2n* elementos. Este protocolo sirve como base para la construcción del grafo *AG* tomando en consideración las medidas preventivas introducidas en el párrafo anterior.

B. K-Anonimato.

En [10] se describe el proceso de transformar una red *G* en una red *AG* con *naive anonymization*. Para evitar que el atacante reconozca los vértices en la red anónima a través de su grado o vecinos, se introduce el concepto de *k-candidato* anónimo. Una red satisface la condición de *k-candidato* anónimo si para cada vértice *v* en el grafo G hay al menos *k* vértices en *AG* que podrían corresponder con *v*.

Dos vértices son automórficamente equivalentes si su estructura dentro de la red es igual. Los vértices que cumplen esta condición pueden permanecer ocultos fácilmente ya que son indistinguibles estructuralmente. Para llevar a cabo un ataque sobre este tipo de vértices, el adversario necesita tener un amplio conocimiento de la red, lo cual puede no ser factible en ciertos tipos de redes.

El grado de conocimiento de la red por parte de un adversario proviene de dos tipos de consultas:

1) Consultas de requerimiento de vértices: proporcionan la información estructural de un vértice en la red.
   a. $\mathcal{H}_0(v)$ proporciona el nombre de *v*,
   b. $\mathcal{H}_1(v)$ proporciona el grado,
   c. $\mathcal{H}_2(v)$ proporciona una lista con el grado de cada vecino del vértice *v*;
2) Consultas para el conocimiento del subgrafo: verifican la existencia de un subgrafo específico en torno al vértice *v*.

A través de este tipo de consultas, en [10] se plantean ataques a tres redes diferentes, y los resultados muestran que gran parte de la información del grafo queda al descubierto para el atacante.

La técnica propuesta para construir la red anónima establece una secuencia de *m* relaciones eliminadas seguidas de *m* relaciones agregadas en el grafo *G*. Las relaciones eliminadas se eligen aleatoriamente (uniformemente) del conjunto de relaciones del grafo original. En este modelo se asume que el atacante sólo ataca un vértice a la vez, y que realiza el análisis estructural para identificar ese vértice a través de sus relaciones. De este estudio se derivan diversas interrogantes concernientes a las estrategias que podrían utilizar los atacantes para la óptima recolección de información: Dado un número limitado de tiempo y recursos, ¿podría el adversario obtener información estructural acerca de un vértice o información de sus atributos? Cuando se está recolectando información estructural, ¿cómo selecciona el atacante el siguiente vértice a explorar? De las conclusiones de [10] se destaca la relación inversamente proporcional entre el grado de anonimato y la utilidad de grafo *AG* obtenido tras modificación aleatoria de *G*.

C. K-Vecindario Anonimato.

En [8] se ejemplifica el llamado ataque de vecindario. Esta idea está relacionada con las consultas para conocimiento de subgrafos descritas en el apartado anterior donde se busca el conjunto de vecinos de un vértice *v* en *G*, para identificarlo posteriormente en la red anónima *AG*. Recordemos que se pretende proteger la privacidad de un grafo con la técnica *k-anónima*, de forma que para cada vértice *v* existen por lo menos $k-1$ vértices con igual grado. Decimos que un grafo cumple con la condición de *k-vecindario* si todos sus vértices cumplen la condición de *k-anónima*.

Se define un grafo simple como:

$$G = (V, E, L, \mathcal{L}),$$

donde *V* es el conjunto de vértices, *E* corresponde al conjunto de aristas en $V \times V$, *L* es el conjunto de etiquetas, y la función de etiquetado que asigna a cada vértice su etiqueta correspondiente es $\mathcal{L}: V \rightarrow L$.

Un vértice es *k-anónimo* en un grafo G si existen al menos otros $(k - 1)$ vértices $v_1,\ldots, v_{k-1} \in V_G$ tal que todos los subgrafos construidos por los vecinos de $v_1 ,\ldots, v_{k-1}$ tienen la misma estructura.

Dado un grafo $G = (V_G, E_G)$ y un entero k, el objetivo es construir un nuevo grafo $AG = (V_{AG}, E_{AG})$ tal que AG sea *k-vecindario* anónimo, y donde $V_{AG} = V_G$, $E_{AG} \supseteq E_G$.

Existen dos formas de anonimizar los vecindarios de vértices: generalizando las etiquetas de vértices y agregando aristas. Por ejemplo, si tenemos una red social donde cada vértice representa a un autor y las aristas ligadas a dos vértices indican que han sido coautores por lo menos en un artículo. Para generalizar las etiquetas de los vértices sería necesario quitar los nombres de los autores y utilizar en su lugar, por ejemplo, el nombre de la institución a la que pertenecen. Añadir aristas permite cumplir con la condición de *k-vecindario*. Ambos métodos generan un costo de anonimización y se elige el que menor costo deriva su aplicación. El costo de anonimización en dos vértices u y v mide la semejanza entre $Vecindario_G\ (u)$ y $Vecindario_G\ (v)$. Cuanto menor sea el costo, más similitudes tendrán ambos vecindarios.

En este escenario no se añaden vértices falsos para mantener la estructura global de la red social, y las aristas del grafo G se mantienen en su versión anónima AG. El método para construir AG consiste en dos pasos. Primero, se extraen los vecindarios de todos los vértices en G (para facilitar la comparación entre vecindarios de diferentes vértices se propone una técnica de codificación de componentes de vecindario). El segundo paso consiste en organizar los vértices en grupos, iniciando la anonimización con los de grado mayor. Al anonimizar vecindarios similares se minimiza la pérdida de información en la transformación de G a AG y se preserva cierta similitud entre la red original y anónima.

Las conclusiones derivadas de la aplicación de este algoritmo a un conjunto de datos sintéticos destacan que el costo del anonimato se incrementa con el número de vértices en el grafo y con el parámetro k (dado que el proceso de anonimización de un vértice requiere que haya otros k vértices con idéntica estructura de conexiones). Por último, cuando la conectividad de los vértices se incrementa, el costo de anonimato crece también. Como trabajo futuro se plantea resolver d-vecindarios donde (d >1), ya que sólo se modeló el problema de 1-vecindarios.

D. K- grado anonimato.

En [11], se propone armar un grafo anónimo AG con el mínimo de modificaciones sobre el grafo original G, a fin de preservar su utilidad como representación de G. Considérese un grafo simple G (V, E), donde V es el conjunto de vértices y E el conjunto de aristas en G; dado un grafo G y un entero k, modifique G para construir AG con *k-grado* anónimo, en donde por cada vértice v existan al menos $k - 1$ vértices de igual grado. La *secuencia de grados* de G se denota como d_G, y es un vector de tamaño $n = |V|$ que contiene los grados de cada vértice en G.

Un grafo G (V, E) cumple con la condición de *k-grado* anónimo si la secuencia de grados del grafo G, llamada d_G, es *k-anónimo*. El costo que conlleva el proceso de hacer un grafo anónimo se define como $G_A\ (AG, G) = |E_{AG}| - |E_G|$.

Los objetivos planteados son: 1) encontrar el *k-grado* anónimo para el grafo; 2) minimizar el costo G_A; 3) mantener una estructura similar de G en AG ($V_{AG} = V_G$).

Se asume el manejo de grafos simples, es decir sin dirección, peso, y donde no se permiten las conexiones de un vértice a sí mismo, ni múltiples conexiones entre un par de vértices. Para minimizar el número de conexiones adicionales se persigue minimizar la distancia L_1 entre la secuencia de grados de G y AG; donde $L_1\ (d_{AG} - d_G) = \sum_i \ |d_{AG}(i) - d_G(i)|$, ya que $|E_{AG}| - |E_G| = ½\ L_1\ (d_{AG} - d_G)$. El modelo permite cierta flexibilidad al formar el grafo anónimo, llamada versión "relajada", la cual no cumple estrictamente la condición de igualdad en la estructura, y se conforma con que sea similar. De esta manera la intersección del conjunto de conexiones es: a) $E_{AG} \cap E_G = E_G$ en la versión estricta; y b) $E_{AG} \cap E_G \approx E_G$ para la versión relajada. De esta observación se deriva el siguiente algoritmo:

1. A partir de la secuencia de grados original d_G, se construye una nueva secuencia de grados d' que sea *k*-anónima, minimizando al mismo tiempo el costo L_1 (d'-d_G)
2. Dada la nueva secuencia de grados d', se construye un grafo AG (V, E) tal que d_{AG} = d', $V_{AG} = V_G$ y $E_{AG} \cap E_G = E_G$ ($E_{AG} \cap E_G = \approx E_G$ para la versión relajada)

El primer paso es resuelto por un algoritmo de programación dinámica de tiempo lineal, mientras que en el segundo se aplica un conjunto de algoritmos de construcción de grafos [11]. En pruebas realizadas en redes sociales con datos reales y sintéticos, se demuestra que los algoritmos son eficientes y preservan la utilidad del grafo mientras satisfacen la condición de *k-grado* anónimo. En las conclusiones también se enfatiza lo complicado de medir con exactitud el grado de información perdida puesto que no existen métricas efectivas para tal problema.

V. CONCLUSIONES

En este documento describimos los métodos y algoritmos que han sido propuestos para anonimizar redes sociales, y los ataques con los que se puede descubrir la identidad de los usuarios que la componen. De acuerdo con los resultados revisados, podemos concluir que los protocolos de anonimizacion propuestos hasta ahora consideran escenarios muy específicos, y que por tanto no pueden aplicarse para la protección de redes sociales genéricas.

Pudimos notar que para efectuar un ataque activo es necesario que la red permita agregar vértices en los lugares escogidos por el adversario, algo que puede no ser realista en muchos casos prácticos.

Una tarea prioritaria es sin duda, desarrollar métricas que permitan evaluar el grado de información perdida en el proceso de anonimización, de forma que se puedan establecer compromisos entre el grado de protección de los vértices y la utilidad de la versión anónima de la red.

REFERENCIAS

[1] J. Imizcoz, *Introducción actores sociales y redes de relaciones: reflexiones para una historia global.* Bilbao: Universidad del País Vasco, 2001, pp. 19-30.

[2] Joshua R. Tyler, Dennis M. Wilkinson, Bernardo A. Huberman, Email as spectroscopy: automated discovery of community structure within organizations, in *Proceedings of Communities and technologies*, 2003, pp. 81-96.

[3] Culotta, R. Bekkerman, A. McCallum. Extracting social networks and contact information from email and the web,in *Proceedings of CEAS-1*, 2004.

[4] Van Alstyne, M. and Zhang, J. 2003. "EmailNet: automatically mining social networks from organizational email communications", in *Proceedings of Annual Conference of the North American Association for Computational Social and Organizational Sciences* (NAACSOS'03), Pittsburg, PA, 2003.

[5] A. Anderson, M. Corney, O. de Vel, and G. Mohay. *Identifying the Authors of Suspect E-mail*, Communications of the ACM, 2001

[6] A. McCallum, X. Wang, and A. Corrada-Emmanuel. *Topic and Role Discovery in Social Networks*, Journal of Artificial Intelligence Research 30, 2007, pp. 249-272.

[7] L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou R3579X?: Anonymized social networks, hidden patterns, and structural steganography. In *Proceedings of the 16th International Conference on World Wide Web (WWW'07)*, pp. 181–190, Alberta, Canada, May 2007.

[8] B. Zhou and J. Pei. Preserving privacy in social networks against neighborhood attacks, in *Proceedings of the 24th International Conference on Data Engineering (ICDE'08)*, Cancun, Mexico, April 2008.

[9] K. Frikken and P. Golle. Private social network analysis: How to assemble pieces of a graph privately. In *Proceedings of the 5th, ACM Workshop on Privacy in Electronic Society (WPES'06)*, pp. 89–98, Alexandria, VA, 2006.

[10] M. Hay, G. Miklau, D. Jensen, P. Weis, and S. Srivastava. "Anonymizing social networks". Technical report, University of Massachusetts Amherst, 2007.

[11] K. Liu and E. Terzi. Towards identity anonymization on graphs, in *Proceedings of ACM SIGMOD*, Vancouver, Canada, June 2008.

[12] A. Acquisti, and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook, in *Proceedings of 6th Workshop on Privacy Enhancing Technologies* (pp. 36-58).

[13] Ed, Giles Hogben, *Security Issues and Recommendations in Online Social Networks*, ENISA Position Paper, Oct 2007.

[14] Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. EPIC. (http://www.privacyinternational.org/)

[15] http://www.rsf.org/article.php3?id_article=10615